FSA IT Security and Privacy Policy Matrix					
Document Source	**Section Number**	**Requirement**	**Test Procedures**	**Y/N/NA/Waived**	**Notes**
FSA ITSPP	2.1, para 2 **Risk Management**	Was the information processed by the system analyzed to determine its level of sensitivity?	**Interview:**		
FSA ITSPP	2.1, para 2 **Risk Management**	Did the sensitivity analysis consider the criticality of the system? Did it contain a general description of sensitivity and indicate if the information's sensitivity level is high, medium, or low for the confidentiality, integrity, and availability categories?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.1, para 2 **Risk Management**	(*Only answer if the system processes information subject to the Privacy Act*) Did the SSO document the number and title of the Privacy Act system of records in the system's security plan?	**Documentation Review:**		
FSA ITSPP	2.1, para 3 **Risk Management**	Has information security been incorporated throughout the entire lifecycle of the system?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.1, para 3 **Risk Management**	Did the System Manager budget for and oversee the completion of a risk assessment for the Information Technology (IT) system?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.1, para 3 **Risk Management**	Has the risk assessment been updated every three years at a minimum by an independent evaluator, or whenever a major change occurred to the system.	**Documentation Review:** **Interview:**		
FSA ITSPP	2.1, para 3 **Risk Management**	Does the risk assessment include the name of the assessor and the date the assessment was completed?	**Documentation Review:**		
FSA ITSPP	2.1, para 3 c (1) **Risk Management**	Has the System Manager supervised the risk assessment to ensure that it considers internal and external threats to the confidentiality, integrity and availability of the system and to data supporting FSA's business operations?	**Interview:**		
FSA ITSPP	2.1, para 3 c (2) **Risk Management**	Does the risk assessment determine the effectiveness of any countermeasures or risk mitigations for the system(s) being assessed and does it state whether or not they are adequate?	**Documentation Review:**		
FSA ITSPP	2.1, para 3 c (3) **Risk Management**	Does the risk assessment include a mission/business impact analysis to determine potential effects of unmitigated risks on the mission or business process the IT system supports, to include an estimated degree of harm or loss that could occur if corrective actions are not taken?	**Documentation Review:**		
FSA ITSPP	2.1, para 3 c (4) **Risk Management**	Based on the business impact analysis, does the risk assessment recommend corrective or mitigating actions that would lower the overall risk to the system?	**Documentation Review:**		
FSA ITSPP	2.1, para 3 c (5) **Risk Management**	Does the risk assessment or CAP propose an implementation schedule and milestones with cost estimates for mitigating unacceptable risks?	**Documentation Review:**		
FSA ITSPP	2.1, para 3 c (6) **Risk Management**	Are updates to the system's security plan monitored by the System Manager?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.1, para 3 c (7) **Risk Management**	Has the System Manager maintained a list of known system vulnerabilities, flaws, or weaknesses that could be exploited by the threat source, including those accepted as risk based decisions?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.1, para 4 **Risk Management**	Has the SSO maintained a file of the risk assessment reports and related management approvals?	**Documentation Review:** **Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	2.2, para 1 **Security Control Reviews**	Has periodic management testing and evaluation been conducted to determine the effectiveness of currently implemented security controls?	**Interview:**		
FSA ITSPP	2.2, para 1 **Security Control Reviews**	Are the security controls of the system and any connected system consistent with the FSA IT architecture?	**Interview:**		
FSA ITSPP	2.2, para 2 **Security Control Reviews**	Has the system undergone tests and examinations, (i.e. network scans, penetration testing, etc.) of key controls on a routine basis?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.2, para 2 **Security Control Reviews**	If security incidents or significant weaknesses were found, have remedial or corrective actions been reported to FSA management?	**Interview:**		
FSA ITSPP	2.2, para 3 **Security Control Reviews**	Has the System Manager budgeted for and conducted a routine self-assessment, in NIST 800-26 format, every three years or whenever a major change occurred to the system?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.2, para 3 **Security Control Reviews**	Has the Inspector General or another independent evaluator conducted an independent review of the system?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.2, para 3 **Security Control Reviews**	If so, were the findings from these reviews reported to OMB as required by the Government Information Security Reform Act (GISRA)?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.3, para 1 **System Security Plan**	Does the system have an approved system security plan, written in the format and containing the topics prescribed in NIST Special Publication 800-18?	**Review Documentation:** **Interview:**		
FSA ITSPP	2.3, para 1 **System Security Plan**	Does the system security plan describe the system and its relationship with all interconnected systems?	**Documentation Review:**		
FSA ITSPP	2.3, para 1 **System Security Plan**	Does the system security plan contain a synopses of supporting documents (i.e. Disaster Recover Plan, Configuration Management Plan, etc,) or contain these supporting documents as appendices?	**Documentation Review:**		
FSA ITSPP	2.3, para 1 **System Security Plan**	Has the SSO reviewed and updated the security plan at least annually to reflect current conditions and risks?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.3, para 1 **System Security Plan**	Is the security plan dated to ease tracking of modifications and approvals?	**Documentation Review:**		
FSA ITSPP	2.4, para 1 **Rules of Behavior**	Has the System Manager established a written Rules of Behavior for the system?	**Documentation Review:**		
FSA ITSPP	2.4, para 1 **Rules of Behavior**	Do the Rules of Behavior reflect administrative as well as technical security controls?	**Documentation Review:**		
FSA ITSPP	2.4, para 1 **Rules of Behavior**	Do the Rules of Behavior delineate responsibilities, primarily detailing the expected behavior of all individuals with access to the system and defining penalties for violation of those behaviors?	**Documentation Review:**		
FSA ITSPP	2.4, para 1 **Rules of Behavior**	Have the Rules of Behavior been published, distributed, and signed by every developer, maintainer, and user of the system?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.4, para 1 **Rules of Behavior**	Do the Rules of Behavior contain procedures for friendly and unfriendly termination of employment?	**Documentation Review:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	2.4, para 2 c (1) **Rules of Behavior**	Do the Rules of Behavior address: working at home?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (2) **Rules of Behavior**	the protection of Privacy Act information?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (3) **Rules of Behavior**	reporting violations?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (4) **Rules of Behavior**	dial-in access?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (5) **Rules of Behavior**	consent to monitoring?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (6) **Rules of Behavior**	connection to the Internet?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (7) **Rules of Behavior**	use of copyrighted works?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (8) **Rules of Behavior**	limitations on the unofficial use of government equipment?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (9) **Rules of Behavior**	the assignment and limitation of system privileges?	**Documentation Review:**		
FSA ITSPP	2.4, para 2 c (10) **Rules of Behavior**	individual accountability, and the consequences for violating the rules of behavior?	**Documentation Review:**		
FSA ITSPP	2.5, para 1 **Solution Life Cycle**	Does the system follow the FSA Security Process Guide (located in the FSA Solution Lifecycle Document as an appendix)?	**Documentation Review:**		
FSA ITSPP	2.5, para 1 **Solution Life Cycle**	Has the SSO completed the corresponding security requirements checklist at the conclusion of each lifecycle phase?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.5, para 1 **Solution Life Cycle**	Is the security checklist complete and has it been signed by the SSO and SM before proceeding to the next lifecycle phase?	**Documentation Review:**		
FSA ITSPP	2.6, para 1 **Certification and Accreditation**	Has the system undergone Certification and Accreditation or received an IATO before becoming operational?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.7, para 1 **Security and Privacy Awareness Training**	Has the System Manager monitored and documented the training of information security personnel who support their system?	**Interview:**		
FSA ITSPP	2.7, para 2 **Security and Privacy Awareness Training**	Have FSA employees received annual information security awareness training that is adequate to fulfill his or her security responsibilities?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.8, para 1 **System Interconnections**	Has the system owner authorized all Memoranda of Understanding (MOU) or Memoranda of Agreement (MOA) between interconnected systems?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.8, para 1 **System Interconnections**	Does the system have a network diagram and documentation for any interconnected systems included within the System's Security Plan?	**Documentation Review:** **Interview:**		
FSA ITSPP	2.8, para 2 c (1) **System Interconnections**	When obtaining system support or development services, does FSA's contract agreement include: how legal security and privacy requirements are met?	**Documentation Review:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	2.8, para 2 c (2) **System Interconnections**	physical and logical controls used to restrict and limit access to sensitive information for only authorized users?	**Documentation Review:**		
FSA ITSPP	2.8, para 2 c (3) **System Interconnections**	the expected availability of services to be maintained in the event of a natural disaster or other interruption of normal processing?	**Documentation Review:**		
FSA ITSPP	2.8, para 2 c (4) **System Interconnections**	the levels of physical security for outsourced equipment?	**Documentation Review:**		
FSA ITSPP	2.8, para 2 c (5) **System Interconnections**	FSA's right to audit?	**Documentation Review:**		
FSA ITSPP	2.8, para 2 c (6) **System Interconnections**	security screening of contractor personnel and security training requirements for contractor personnel?	**Documentation Review:**		
FSA ITSPP	2.8, para 2 c (7) **System Interconnections**	language requiring a contractor to inform the system manager and SSO when contract personnel depart from the contract?	**Documentation Review:**		

FSA IT Security and Privacy Policy Matrix					
Document Source	**Section Number**	**Requirement**	**Test Procedures**	**Y/N/NA/Waived**	**Notes**
FSA ITSPP	3.1.1, para 1 **Personnel Security: Establishing and Terminating Accounts**	Does the SSO use a documented process for requesting, establishing, issuing, and closing all user accounts?	**Documentation Review:** **Interview:**		
FSA ITSPP	3.1.1, para 1 **Personnel Security: Establishing and Terminating Accounts**	Does this process include linkages to the human resource and contracting functions involved in new hires, transfers, contract award, oversight, and termination of employment?	**Interview:**		
FSA ITSPP	3.1.1, para 1 **Personnel Security**	Are all user accounts current and reviewed regularly?	**Interview:**		
FSA ITSPP	3.1.1, para 2 **Personnel Security: Establishing and Terminating Accounts**	Has the SSO, or designee, identified any system privileges or features, which would allow a user to override system or application controls, and associate these privileges with the categories of staff that would use them?	**Interview:**		
FSA ITSPP	3.1.1, para 2 **Personnel Security: Establishing and Terminating Accounts**	Has the SSO maintained an authorization process and record of privileges?	**Documentation Review:** **Interview:**		
FSA ITSPP	3.1.1, para 2 **Personnel Security: Establishing and Terminating Accounts**	Has the SSO reviewed authorization for privileged access rights at least quarterly to see if privileged access is still required, and to make sure users have not been erroneously assigned unauthorized privileges?	**Interview:**		
FSA ITSPP	3.1.2, para 1 **Personnel Security: Position Descriptions**	Has the System Manager established job descriptions that accurately document assigned duties and responsibilities?	**Documentation Review:** **Interview:**		
FSA ITSPP	3.1.3, para 1 **Personnel Security: Sensitivity/Risk Levels**	Has the System Manager classified the sensitivity of each position?	**Interview:**		
FSA ITSPP	3.1.4, para 1 **Personnel Security: Background Screening**	Have FSA employees or contractors undergone an appropriate background screening for his or her assigned positions prior to obtaining access to the system?	**Interview:**		
FSA ITSPP	3.1.4, para 1 **Personnel Security: Background Screening**	Have screenings, both clearances and investigations, been renewed at least every five years?	**Interview:**		
FSA ITSPP	3.1.4, para 2 **Personnel Security: Background Screening**	Is there documentation describing the conditions for access to the system, especially when it is necessary to grant access prior to the completion of a background screening?	**Documentation Review:**		
FSA ITSPP	3.1.4, para 2 **Personnel Security: Background Screening**	Does the documentation state which compensating controls (e.g. accompanying an individual in a sensitive area) will be used to mitigate associated risk of granting access to unscreened personnel?	**Documentation Review:**		
FSA ITSPP	3.1.5, para 1 **Personnel Security: Use of External Connections**	When appropriate, do terms and conditions of employment state that security responsibilities extend outside of the workplace (e.g. telecommuting, travel, etc)?	**Documentation Review:** **Interview**		
FSA ITSPP	3.1.5, para 1 **Personnel Security: Use of External Connections**	Has the System Manager approved all external connections in advance, and complied with FSA security standards?	**Interview**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.1.6, para 1 **Personnel Security: Nondisclosure and Confidentiality Agreements**	Have all FSA employees and contractors that access sensitive information signed a nondisclosure and/or confidentiality agreement covering the privileged/sensitive data or information with which they will come in contact by accessing FSA networks?	**Documentation Review:** **Interview**		
FSA ITSPP	3.1.6, para 1 **Personnel Security: Nondisclosure and Confidentiality Agreements**	Do the annual Information Security Awareness Briefings reemphasize the nondisclosure and confidentiality agreements?	**Interview**		
FSA ITSPP	3.1.7, para 1 **Personnel Security: Segregation of Duties**	Has the System Manager created formal procedures defining the authority granted to each user or class of users?	**Documentation Review:** **Interview**		
FSA ITSPP	3.1.7, para 1 **Personnel Security: Segregation of Duties**	Have users received only the minimum access(es) necessary to perform their jobs?	**Interview**		
FSA ITSPP	3.1.7, para 1 **Personnel Security: Segregation of Duties**	Have development, test and operational facilities been separated to support the segregation of duties and prevent unwanted alteration or modification of operational systems?	**Interview**		
FSA ITSPP	3.1.7, para 1 **Personnel Security: Segregation of Duties**	Do at least two people possess expertise in every important computer, network or telecommunications related area?	**Interview**		
FSA ITSPP	3.1.7, para 1 **Personnel Security: Segregation of Duties**	Do key personnel take regularly scheduled vacations and periodically rotate job/shift responsibilities?	**Interview**		
FSA ITSPP	3.1.8, para 1 **Personnel Security: Compliance**	On at least an annual basis, has the System Manager validated compliance with personnel security controls for all personnel under their supervision?	**Interview**		
FSA ITSPP	3.2.1, para 1 **Physical and Environmental Protection: Physical Access Controls**	Does FSA control access to facilities and rooms that house systems through the use of guards, identification badges, and/or entry devices such as keycards to prevent unauthorized entry?	**Interview**		
FSA ITSPP	3.2.1, para 1 **Physical and Environmental Protection: Physical Access Controls**	Are there established emergency exit and reentry procedures to protect assets during an emergency and to prevent unauthorized reentry into facilities after the emergency expires?	**Documentation Review:** **Interview**		
FSA ITSPP	3.2.1, para 1 **Physical and Environmental Protection: Physical Access Controls**	Do facility personnel securely store unused keys, keycards or other entry devices used to enter sensitive areas and return these devices when no longer needed?	**Interview**		
FSA ITSPP	3.2.1, para 2 **Physical and Environmental Protection: Physical Access Controls**	Do all personnel have and display their identification badges at all times, regardless of the area's sensitivity?	**Interview** **Visual Inspection**		
FSA ITSPP	3.2.1, para 2 **Physical and Environmental Protection: Physical Access Controls**	Do all facility personnel authenticate visitors, contractors, and maintenance personnel through the use of preplanned appointments and identification checks, and do they escort these persons when in restricted or sensitive areas?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.2.1, para 3 **Physical and Environmental Protection: Physical Access Controls**	Do restricted or sensitive areas have clearly defined security perimeters, with appropriate access controls?	**Interview:** **Visual Inspection:**		
FSA ITSPP	3.2.1, para 3 **Physical and Environmental Protection: Physical Access Controls**	Are audit logs reviewed periodically for suspicious activity?	**Interview:**		
FSA ITSPP	3.2.1, para 3 **Physical and Environmental Protection: Physical Access Controls**	Do facility personnel change entry codes periodically?	**Interview:**		
FSA ITSPP	3.2.1, para 3 **Physical and Environmental Protection: Physical Access Controls**	Do FSA management and supervisors regularly review the list of persons with physical access to these areas?	**Interview:**		
FSA ITSPP	3.2.1, para 3 **Personnel Security: Physical Access Controls**	Do personnel report and investigate all suspicious activity and/or security violations?	**Interview:**		
FSA ITSPP	3.2.1, para 4 **Physical and Environmental Protection: Physical Access Controls**	Do personnel and contractors position computer monitors displaying sensitive data in areas that prevent viewing by unauthorized personnel?	**Interview:** **Visual Inspection:**		
FSA ITSPP	3.2.1, para 4 **Physical and Environmental Protection: Physical Access Controls**	Do facility personnel restrict and monitor physical access to data and telecommunication transmission lines and their housing facilities?	**Interview:**		
FSA ITSPP	3.2.1, para 4 **Physical and Environmental Protection: Physical Access Controls**	In the case of portable/mobile devices, do personnel encrypt data files that contain information designated as "sensitive"?	**Interview:**		
FSA ITSPP	3.2.2, para 1 **Physical and Environmental Protection: Physical Access Controls**	Does FSA maintain and periodically review its environmental assets, such as electric power distribution nodes and lines, heating/air conditioning facilities and units, water pipes, etc. for risk of failure?	**Interview:**		
FSA ITSPP	3.2.2, para 1 **Physical and Environmental Protection: Physical Access Controls**	Do facilities provide uninterruptible power supplies or backup generators to areas that support critical and/or sensitive systems?	**Interview:** **Visual Inspection:**		
FSA ITSPP	3.3, para 1 **Production Input/Output Controls**	Are there procedures for the system that address controlling system production inputs and outputs?	**Documentation Review:** **Interview**		
FSA ITSPP	3.3, para 1 **Production Input/Output Controls**	Does every system user have access to a help desk or other user support system capable of providing assistance to authorized users of the system in the event of an input/output incident?	**Interview:**		
FSA ITSPP	3.3, para 2 **Production Input/Output Controls**	Does FSA externally label all media for sensitivity and include any special handling instructions on the label?	**Interview:** **Visual Inspection:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.3, para 3 **Production Input/Output Controls**	Is the movement of sensitive media from or into storage or restricted areas logged and is an audit trail maintained to record all such movements?	**Documentation Review:** **Interview**		
FSA ITSPP	3.3, para 3 **Production Input/Output Controls**	Do security personnel have established and maintained controls for transporting or mailing media or printed output?	**Interview:**		
FSA ITSPP	3.3, para 4 **Production Input/Output Controls**	Are there procedures established for shredding or destroying sensitive hardcopy media when no longer needed or when damaged/spoiled, including:	**Documentation Review:** **Interview**		
FSA ITSPP	3.3, para 4 **Personnel Security: Production Input/Output Controls**	a logging form to keep track of the destruction?	**Documentation Review:** **Interview**		
FSA ITSPP	3.3, para 4 **Personnel Security: Production Input/Output Controls**	Are there procedures established for sanitizing electronic media for reuse, storage or destruction when no longer needed or if it becomes damaged/spoiled?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4, para 1 **Contingency Planning**	Does the system's Contingency Plan define emergency operating procedures to be followed for critical functions to continue in order to operate and support the system in the event of disruptions, both large and small?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4, para 1 **Contingency Planning**	Do the emergency procedures have timelines for recovery and restoration of specified services prioritized by the system's mission criticality?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4, para 1 **Contingency Planning**	Are the test backup and restoration procedures regularly review?	**Interview:**		
FSA ITSPP	3.4, para 3 **Contingency Planning**	Is there a comprehensive contingency and disaster recovery plan in place for the system that has been tested?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4, para 3 **Contingency Planning**	Does this plan have detailed procedures for restoring operation of the system, including the personnel responsible and the timeline within which the system must be returned to normal business operations?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4, para 3 **Contingency Planning**	Are there personnel responsible to execute contingency procedures trained in their duties?	**Interview:**		
FSA ITSPP	3.4, para 4 **Contingency Planning**	Has the SSO for the system completed a comprehensive contingency plan prior to authorizing the system for processing?	**Interview:**		
FSA ITSPP	3.4, para 4 **Contingency Planning**	Does the contingency plan incorporate the results of the latest Risk Assessments to focus attention on the likeliest disrupting events?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4, para 4 **Contingency Planning**	Has the SSO distributed the contingency plan to the appropriate personnel?	**Interview:**		
FSA ITSPP	3.4.1, para 1 **Contingency Planning: Plan Maintenance**	Does the contingency plan specify conditions necessary for activating the plan and who is to be involved in the activation decision?	**Documentation Review:**		
FSA ITSPP	3.4.1, para 1 **Contingency Planning: Plan Maintenance**	Have the system manager, SSO, and CSO reviewed and approved the contingency plan?	**Interview:**		
FSA ITSPP	3.4.1, para 1 **Contingency Planning: Plan Maintenance**	Are the plans stored at a secure offsite facility along with all necessary documentation for operating and/or restoring the system?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.4.1, para 1 **Contingency Planning: Plan Maintenance**	Are copies of key vendor contracts that impact the operation or restoration of core FSA functions maintained at this location?	**Interview:**		
FSA ITSPP	3.4.1, para 2 **Contingency Planning: Plan Maintenance**	Has the System Manager conducted and documented tests of their contingency/disaster recovery plans at least annually?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4.1, para 2 **Contingency Planning: Plan Maintenance**	Has the system manager informed the Designated Accrediting Authority (DAA) of the results of the testing and any resulting readjustments to the plans?	**Interview:**		
FSA ITSPP	3.4.2, para 1 **Contingency Planning: Alternate Site Capability**	Has the System Manager planned for the use of a secure alternate processing site geographically removed from its primary site?	**Interview:**		
FSA ITSPP	3.4.3, para 1 **Contingency Planning: System Backup**	Does the system have documented backup procedures, which include frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and/or differential backup)?	**Documentation Review:** **Interview**		
FSA ITSPP	3.4.3, para 1 **Contingency Planning: System Backup**	Do the system operators backup all systems critical data files nightly and move the files to a geographically separate location each day?	**Interview:**		
FSA ITSPP	3.4.3, para 1 **Contingency Planning: System Backup**	Are full system backups completed at least weekly?	**Interview:**		
FSA ITSPP	3.4.3, para 1 **Contingency Planning: System Backup**	Are at least three generations/cycles of backup information retained for mission critical or mission important systems?	**Interview:**		
FSA ITSPP	3.5, para 1 **Data Integrity**	Are there data integrity procedures that describe how the system detects and prevents any unauthorized alteration or destruction of data, caused by either malicious or accidental means?	**Documentation Review:** **Interview**		
FSA ITSPP	3.5.1, para 1 **Data Integrity: Virus Detection and Elimination**	Is virus detection and elimination software installed on the system?	**Interview:** **Technical Inspection:**		
FSA ITSPP	3.5.1, para 1 **Data Integrity: Virus Detection and Elimination**	Are there procedures established that address routine updates to virus signature files, including automatic and/or manual virus scans?	**Interview:**		
FSA ITSPP	3.5.1, para 1 **Data Integrity: Virus Detection and Elimination**	Does the virus scanning include screening non-text files?	**Interview:** **Technical Inspection:**		
FSA ITSPP	3.5.2, para 1 **Data Integrity: Verification**	Does the system use integrity verification programs that meet the integrity requirements of the system?	**Interview:** **Technical Inspection:**		
FSA ITSPP	3.5.2, para 1 **Data Integrity: Verification**	Do the verification programs look for evidence of deliberate acts such as data tampering, as well as data entry errors, corruption of correctly entered data and omissions?	**Interview:**		
FSA ITSPP	3.5.3, para 1 **Data Integrity: Reconciliation**	Are there procedures established that address reconciling data transfers, including a description of the actions taken to resolve any discrepancies?	**Documentation Review:** **Interview**		
FSA ITSPP	3.5.4, para 1 **Data Integrity: Message Authentication**	If the system has requirements for non-repudiation and medium or high integrity does it also have written procedures describing the use of message authentication?	**Documentation Review:** **Interview**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.5.4, para 1 **Data Integrity: Message Authentication**	Have personnel reviewed these procedures at least annually to sustain their continued validity?	**Interview:**		
FSA ITSPP	3.5.5, para 1 **Data Integrity: Performance Measurements**	Is system performance monitoring used to create and analyze system performance logs for availability problems, including active attacks and system and network slowdowns and crashes?	**Interview:**		
FSA ITSPP	3.5.5, para 1 **Data Integrity: Performance Measurements**	Do personnel analyze performance logs on a near real-time basis?	**Interview:**		
FSA ITSPP	3.5.5, para 1 **Data Integrity: Performance Measurements**	If so, are there written procedures established that address near real-time performance analysis?	**Documentation Review:** **Interview**		
FSA ITSPP	3.5.5, para 1 **Data Integrity: Performance Measurements**	Has the System Manager identified whether the system can operate at the required availability level while using periodic performance sampling or other less demanding controls?	**Interview:**		
FSA ITSPP	3.5.5, para 1 **Data Integrity: Performance Measurements**	Does the System Manager review these procedures at least annually?	**Interview:**		
FSA ITSPP	3.5.6, para 1 **Data Integrity: Intrusion Detection**	Does the System Manager monitor the current status of intrusion detection tools on the information system and networks for which they are responsible?	**Interview:**		
FSA ITSPP	3.5.6, para 1 **Data Integrity: Intrusion Detection**	Do systems' personnel inform the system's owner whenever intrusion detection tools are implemented or modified?	**Interview:**		
FSA ITSPP	3.5.6, para 1 **Data Integrity: Intrusion Detection**	Do the records include a description of intrusion detection tools installed on the system, where they are placed, the type of processes detected/reported, and the handling procedures?	**Documentation Review:** **Interview**		
FSA ITSPP	3.5.6, para 1 **Data Integrity: Intrusion Detection**	Are system logs reviewed for anomalies on a daily basis, using automated or manual methods?	**Interview:**		
FSA ITSPP	3.5.6, para 1 **Data Integrity: Intrusion Detection**	Does the System Manger routinely review intrusion detection reports after suspected incidents, and assign responsibility for incident resolution and lessons learned?	**Interview:**		
FSA ITSPP	3.5.6, para 2 **Data Integrity: Intrusion Detection**	Does the System Manager conduct periodic reviews on the software and data content of the systems for which they are responsible?	**Interview:**		
FSA ITSPP	3.5.6, para 2 **Data Integrity: Intrusion Detection**	Are all unapproved files or amendments discovered during such reviews subject to a formal review process to determine the level of risk that such unapproved software/data content represents, and the extent to which intrusion detection or other tools may not have adequately performed in order to alert system operators to unauthorized installation(s)?	**Interview:**		
FSA ITSPP	3.5.6, para 2 **Data Integrity: Intrusion Detection**	Are formal all such reviews formally documented?	**Documentation Review:** **Interview**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.5.7, para 1 **Data Integrity: Penetration Testing**	Are there procedures established for the system to ensure that penetration testing is conducted appropriately and on a periodic basis?	**Documentation Review:** **Interview**		
FSA ITSPP	3.5.7, para 1 **Data Integrity: Penetration Testing**	Has the SSO recorded results of such testing and reported on the ensuing corrective actions?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (1) **Documentation**	Does the system have: a current System Security Plan?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (2) **Documentation**	Certification and Accreditation documents and statements authorizing a system to process, including all required appendices?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (3) **Documentation**	a log of service packs, patches upgrades, etc. for the system, and the order of installation for the FSA Major Application and/or General Support System?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (4) **Documentation**	a Network diagram and documentation on placement and configuration of firewalls, intrusion detection sensors or other security software or appliances?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (5) **Documentation**	standard operating procedures that support all operations of the application or general support system?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (6) **Documentation**	user manuals to explain correct usage of software/hardware?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (7) **Documentation**	vendor-supplied documentation of software and hardware?	**Interview** **Visual Inspection:**		
FSA ITSPP	3.6, para 1 c (8) **Documentation**	application documentation, requirements, and specifications per the system's current contract?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 1 c (9) **Documentation**	software and hardware testing procedures and results?	**Documentation Review:** **Interview**		
FSA ITSPP	3.6, para 2 **Documentation**	Does the SSO know the locations and latest version numbers of all required documentation?	**Interview:**		
FSA ITSPP	3.7, para 1 **Configuration Management**	Has the system manager created a configuration management plan that describes the hardware and system software maintenance controls in place and the process by which configuration controls will be maintained for that system?	**Documentation Review:** **Interview**		
FSA ITSPP	3.7, para 2 **Configuration Management**	Does the plan include an established, systematic process for addressing the introduction of new configurations into systems and networks to make sure software upgrades or security patches work in the intended way and do not adversely impact other security or functionality aspects of the system?	**Documentation Review:** **Interview**		
FSA ITSPP	3.7.1, para 1 **Configuration Management: Configuration Control**	Are there procedures established that address configuration changes unique to the system?	**Interview:**		
FSA ITSPP	3.7.1, para 1 **Configuration Management: Configuration Control**	Is there a formal change control process in place for the system requiring tests and approval for any change before entering into production?	**Interview:**		
FSA ITSPP	3.7.1, para 1 c (1) **Configuration Management: Configuration Control**	Do the procedures state that the system must use software change request forms to document requests and related approvals?	**Documentation Review:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.7.1, para 1 c (2) **Configuration Management: Configuration Control**	Do the procedures state that the system must use version control, allowing association of system components to the appropriate system version?	**Documentation Review:**		
FSA ITSPP	3.7.1, para 1 c (3) **Configuration Management: Configuration Control**	Do the procedures state that the SSOs must attend the configuration control meetings and make recommendations on proposed changes?	**Documentation Review:**		
FSA ITSPP	3.7.1.1, para 1 **Configuration Management: Configuration Control: Change Management**	Has the System Manager made sure that the system follows the configuration management process, including descriptions and enforcement of change identification, approval, and documentation procedures?	**Interview:**		
FSA ITSPP	3.7.1.1, para 1 **Configuration Management: Configuration Control: Change Management**	Has the System Manager made recommendations on the required training needed for both technical and user communities to implement new configurations and controls?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (1) **Configuration Management: Configuration Control: Change Management**	Do change management processes include: an Impact Analysis to determine the affect of proposed changes on existing security controls, including the required training needed to implement the control?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (2) **Configuration Management: Change Management**	documentation of all changes to application software along with the procedures used for testing and/or approving changes to system components prior to proceeding to the production environment?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (3) **Configuration Management: Configuration Control: Change Management**	a specification of the type of test data to be used (live or made-up) in the testing process?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (4) **Configuration Management: Configuration Control: Change Management**	whether live data is to be used, specification of the process for assuring the confidentiality and integrity of the data?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (5) **Configuration Management: Change Management**	documentation of test results and, upon implementation, System Manager's review of the updated detailed system specifications?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (6) **Configuration Management: Configuration Control: Change Management**	documentation describing the distribution and implementation of new or revised software, including effective date for all locations?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (7) **Configuration Management: Configuration Control: Change Management**	consideration of special procedures for performance of emergency repair, emergency maintenance, and interim authorization for processing?	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (8) **Configuration Management: Configuration Control: Change Management**	documentation of emergency change procedures, which must be approved by management within a maximum of five days? These procedures must be dynamic and regularly updated to draw upon actual experiences with emergencies.	**Interview:**		
FSA ITSPP	3.7.1.1, para 2 c (9) **Configuration Management: Configuration Control: Change Management**	updates to system security plans, contingency plan, and other associated documentation?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.7.2, para 1 **Configuration Management: Configuration and Management Documentation**	Are there procedures to restrict or control the activities of those who perform maintenance and repair activities, both on-site and off-site?	**Interview:**		
FSA ITSPP	3.7.2, para 1 **Configuration Management: Configuration and Management Documentation**	Are there specified procedures that reflect issues such as the escort of maintenance personnel, sanitization of devices removed from the site, and other issues relevant to the systems under his/her control?	**Interview:**		
FSA ITSPP	3.7.2.1, para 1 **Configuration Management: Configuration and Management Documentation: Maintenance and Repair**	Has the System Manager reviewed all default security parameters to correlate with system sensitivity requirements?	**Interview:**		
FSA ITSPP	3.7.2.1, para 1 **Configuration Management: Configuration and Management Documentation: Maintenance and Repair**	Are default security settings set to a restrictive setting?	**Interview:** **Technical Inspection:**		
FSA ITSPP	3.7.2.1, para 2 **Configuration Management: Configuration and Management Documentation: Maintenance and Repair**	Are there procedures used to control remote maintenance services?	**Interview:**		
FSA ITSPP	3.7.2.1, para 2 **Configuration Management: Configuration and Management Documentation: Maintenance and Repair**	Has the System Manager implemented access controls and other security precautions to prevent potentially malicious code, such as "back doors," from being used to evade authentication and authorization protections?	**Interview:**		
FSA ITSPP	3.7.2.1, para 2 **Configuration Management: Configuration and Management Documentation: Maintenance and Repair**	Does the implementation of maintenance or repairs take place at such times and under such circumstances so as to minimize impacts to business processes?	**Interview:**		
FSA ITSPP	3.7.2.1, para 3 **Configuration Management: Configuration and Management Documentation: Maintenance and Repair**	Has the System Manager periodically reviewed the system to identify and, when possible, eliminate unnecessary services (e.g. FTP, HTTP, mainframe supervisor calls)?	**Interview:**		
FSA ITSPP	3.7.2.1, para 3 **Configuration Management: Configuration and Management Documentation: Maintenance and Repair**	Has the System Manager periodically reviewed the system for known vulnerabilities and current installation of software patches?	**Interview:**		
FSA ITSPP	3.7.2.2, para 1 **Configuration Management: Configuration and Management Documentation: Unapproved Software**	Does software installation and use follow the principle that whatever is not expressly allowed is denied?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.7.2.2, para 1 **Configuration Management: Configuration and Management Documentation: Unapproved Software**	Are there organizational procedures for dealing with, and protecting against, the inappropriate use of copyrighted software?	**Interview:**		
FSA ITSPP	3.7.2.2, para 1 **Configuration Management: Configuration and Management Documentation: Unapproved Software**	If useing a copyrighted product, have sufficient licensed copies of the software been purchased for the system on which the application will be processed?	**Interview:**		
FSA ITSPP	3.7.2.2, para 2 **Configuration Management: Configuration and Management Documentation: Unapproved Software**	Have periodic audits of FSA computers been performed to make sure users do not install unapproved software?	**Interview:**		
FSA ITSPP	3.7.2.3, para 1 **Configuration Management: Configuration and Management Documentation: Application Ownership**	Do contracts clearly specify whether the government owns the software, whether the software was developed in-house or under contract, or if the application software was received from another federal agency with the understanding that it was federal government property?	**Documentation Review:** **Interview:**		
FSA ITSPP	3.8, para 1 **Incident Response**	Are intrusion detection tools, firewalls, automated audit logs, and other preventative measures used to assist system security staff when a security incident occurs in the system?	**Interview:**		
FSA ITSPP	3.8, para 2 **Incident Response**	Are system security personnel adequately trained to recognize security incidents?	**Interview:**		
FSA ITSPP	3.8, para 2 **Incident Response**	Have procedures for reporting and responding to those incidents been established?	**Interview:**		
FSA ITSPP	3.8, para 2 **Incident Response**	Are incidents monitored and tracked until resolved, and is documentation maintained concerning the incident and its resolution?	**Documentation Review:** **Interview:**		
FSA ITSPP	3.8.1, para 1 **Incident Response: Information Sharing**	Is information regarding incidents and common vulnerabilities or threats shared with system personnel and appropriate managers of systems and networks interconnected with FSA?	**Interview:**		
FSA ITSPP	3.8.1, para 2 **Incident Response: Information Sharing**	Does FSA management assign specific individual(s) to receive and respond to alerts/advisories, vendor patches, exploited vulnerabilities, etc?	**Interview:**		
FSA ITSPP	3.8.2, para 2 **Incident Response: Information Sharing**	Do users notify System Managers and/or system administrators as soon as possible about any observed or suspected security weaknesses in, or threats to, systems or services?	**Interview:**		
FSA ITSPP	3.8.2, para 2 **Incident Response: Information Sharing**	Do users report software malfunctions and report the malfunction using the same procedures?	**Interview:**		
FSA ITSPP	3.8.2, para 3 **Incident Response: Information Sharing**	Does the SSO report incidents to the CSO?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	3.8.3, para 1 **Incident Response: Post Incident Activities**	Does the FSA System Manager review incident handling procedures and control techniques after each incident and, when necessary, modify the procedures to prevent recurrence?	**Interview:**		
FSA ITSPP	3.8.3, para 1 **Incident Response: Post Incident Activities**	Does the FSA System Manager collect and secure audit trails and other tracking mechanisms for analysis and use as potential evidence?	**Interview:**		

FSA IT Security and Privacy Policy Matrix					
Document Source	**Section Number**	**Requirement**	**Test Procedures**	**Y/N/NA/Waived**	**Notes**
FSA ITSPP	4.1, para 1 **Identification and Authentication**	Are there identification and authentication procedures established to prevent unauthorized use or access?	**Interview:**		
FSA ITSPP	4.1, para 1 c (1) **Identification and Authentication**	Before granting initial access to a system, does the SSO verify: that the user has authorization from the system owner to access the system?	**Interview:**		
FSA ITSPP	4.1, para 1 c (2) **Identification and Authentication**	that the level of access is appropriate for the user's business purpose?	**Interview:**		
FSA ITSPP	4.1, para 1 c (3) **Identification and Authentication**	that the access will not compromise segregation of duties?	**Interview:**		
FSA ITSPP	4.1, para 1 c (4) **Identification and Authentication**	that the user received a copy of the Rules of Behavior for the system and has signed a statement indicating that he/she understands and agrees to the Rules?	**Interview:**		
FSA ITSPP	4.1, para 1 c (5) **Identification and Authentication**	that the completion (for high-risk positions) or initiation (for low-medium risk positions) of proper background screening?	**Interview:**		
FSA ITSPP	4.1, para 2 **Identification and Authentication**	Does the system correlate actions to users via the creation of unique user IDs for each individual user?	**Interview:**		
FSA ITSPP	4.1, para 2 **Identification and Authentication**	If any user requires special privileges or features beyond their primary job function, which would allow them to override system or application controls, do they use an additional user ID different than that used for normal business purposes?	**Interview:**		
FSA ITSPP	4.1, para 2 **Identification and Authentication**	Is there documentation describing whether passwords, tokens, biometrics or other methods are used for access purposes and how the access control mechanisms will support individual accountability and audit trails for the system?	**Documentation Review:** **Interview**		
FSA ITSPP	4.1, para 3 **Identification and Authentication**	Are there security controls in place that are able to detect unauthorized and/or invalid attempts to access the system?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.1, para 3 **Identification and Authentication**	Are the number of invalid access attempts that may occur for a given user ID or access location (i.e. terminal or port) determined and documented?	**Documentation Review:** **Interview:** **Technical Inspection:**		
FSA ITSPP	4.1, para 3 **Identification and Authentication**	Are the actions taken when that limit is exceeded included in the documentation?	**Documentation Review:** **Interview**		
FSA ITSPP	4.1, para 4 **Identification and Authentication**	If a system allows bypassing of user authentication requirements, (for example, single-sign-on technologies, host-to-host authentication servers, user-to-host identifier, and group user identifiers), does the SSO document the governing procedures, as well as any compensating controls and whether emergency or temporary access is authorized?	**Documentation Review:** **Interview**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.1, para 4 **Identification and Authentication**	Is host-based authentication, granting access based on the identity of the host originating the request instead of the individual user requesting access, permitted to control access?			
FSA ITSPP	4.1, para 4 **Identification and Authentication**	If this method is used on the system, is it documented and are controls put in place to remove access authorization when hosts no longer have legitimate access?			
FSA ITSPP	4.1.1, para 1 **Identification and Authentication: System Login**	Do the login procedures include an appropriate banner containing the following warning: You are about to access a United States government computer network intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution?			
FSA ITSPP	4.1.1, para 1 **Identification and Authentication: System Login**	Does the banner include a "click through" requirement so that the person logging in must agree to the terms before accessing the FSA system?			
FSA ITSPP	4.1.1, para 2 **Identification and Authentication: System Login**	Do the Login procedures limit the amount of information displayed about the system and its functions until after a user has successfully logged in?			
FSA ITSPP	4.1.1, para 2 c (1) **Identification and Authentication: System Login**	Does the system not display: system or application identifiers during login?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.1.1, para 2 c (2) **Identification and Authentication: System Login**	help messages during login?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.1.1, para 2 c (3) **Identification and Authentication: System Login**	validation of any portion of the login information, for example, not indicating which part of the login data was correct or incorrect during login?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.1.1, para 3 **Identification and Authentication: System Login**	Does the system mask a user's password during login?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.1.2, para 1 **Identification and Authentication: Passwords**	If passwords are the access control method used for authentication to the system, has the SSO documented the password procedures for the system?	**Documentation Review:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.1.2, para 1 **Identification and Authentication: Passwords**	Does the documentation include specific information regarding allowable character sets, password length (maximums and minimums), password aging time frames and enforcement approach, and the number of generations of expired passwords disallowed for use?	**Documentation Review:**		
FSA ITSPP	4.1.2, para 1 **Identification and Authentication: Passwords**	Do passwords contain a minimum of eight characters in length and include any combination of the following to meet or exceed FIPS Publication 112 standards: · English uppercase letters (A-Z) · English lowercase letters (a-z) · Westernized Arabic numerals (0-9) · Non-alphanumeric special characters (!, @, #, $, &, *)?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.1.2, para 2 **Identification and Authentication: Passwords**	Were vender-supplied and/or default passwords on the system changed immediately?	**Interview:**		
FSA ITSPP	4.1.2, para 2 **Identification and Authentication: Passwords**	Are users forced to change their passwords immediately upon initial login as a new user?	**Interview:**		
FSA ITSPP	4.1.2, para 2 **Identification and Authentication: Passwords**	Are temporary passwords (if a user forgets a password) only given after positively identifying the user?	**Interview:**		
FSA ITSPP	4.1.2, para 2 **Identification and Authentication: Passwords**	Are users informed not to write down or reveal their passwords to anyone?	**Interview:**		
FSA ITSPP	4.1.2, para 2 **Identification and Authentication: Passwords**	Are there procedures in place for handling lost and/or compromised passwords?	**Interview:**		
FSA ITSPP	4.1.2, para 2 **Identification and Authentication: Passwords**	Are password transmissions or storage encrypted to prevent capture?	**Interview:**		
FSA ITSPP	4.1.2, para 3 **Identification and Authentication: Passwords**	Are there procedures in place describing the creation of emergency passwords?	**Interview:**		
FSA ITSPP	4.1.2, para 3 **Identification and Authentication: Passwords**	Do these procedures include who may authorize, duration of password validity, and criteria for granting emergency access?	**Interview:**		
FSA ITSPP	4.1.2, para 4 **Identification and Authentication: Passwords**	Must users change their passwords at least every ninety days or earlier if needed?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.1.2, para 4 **Identification and Authentication: Passwords**	Does the system have procedures established to enforce password changes and identify who changes their passwords?	**Interview:**		
FSA ITSPP	4.1.2, para 4 **Identification and Authentication: Passwords**	Are there procedures established (such as using password crackers/checkers) to determine compliance with password policy?	**Interview:**		
FSA ITSPP	4.1.2, para 4 **Identification and Authentication: Passwords**	Is the use of such tools limited only to those persons expressly authorized by the system manager?	**Interview:**		
FSA ITSPP	4.1.2, para 4 **Identification and Authentication: Passwords**	Does the System Manager record the authorization and specify the locations, systems and duration covered by the authorization?	**Interview:**		
FSA ITSPP	4.1.2, para 5 **Identification and Authentication: Passwords**	Are there procedures established that describe how the system limits access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, or scripts with embedded passwords are allowed only for specific (i.e. batch, etc.) applications)?	**Documentation Review:**		
FSA ITSPP	4.1.3, para 1 **Identification and Authentication: PKI and Biometrics**	Does the use of Public Key Infrastructure (PKI) technology conform to FIPS 186-2, Digital Signature Standard, and FIPS 180-1, Secure Hash Standard, issued by NIST, unless the system manager grants a waiver?	**Documentation Review:**		
FSA ITSPP	4.1.3, para 1 **Identification and Authentication: PKI and Biometrics**	Are there procedures established describing cryptographic key management processes for key generation, distribution, storage, entry, use, destruction, and archiving?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.1.3, para 2 **Identification and Authentication: PKI and Biometrics**	Does documentation exist for the system describing whether encryption is used to prevent unauthorized access to sensitive data transfers?	**Documentation Review:**		
FSA ITSPP	4.1.3, para 2 **Identification and Authentication: PKI and Biometrics**	If PKI is used, has the system manager created procedures detailing how PKI certificates are generated and controlled?	**Interview:**		
FSA ITSPP	4.1.3, para 2 **Identification and Authentication: PKI and Biometrics**	If encryption is used primarily for authentication, has the SSO included this information in the encryption documentation?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.1.3, para 3 **Identification and Authentication: PKI and Biometrics**	If the system uses biometrics and/or tokens, is there documentation that describes the controls being used and how they are implemented on the system?	**Documentation Review:** **Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.1.3, para 3 **Identification and Authentication: PKI and Biometrics**	If the system uses biometrics and/or tokens, does the documentation indicate if any special hardware (such as card readers) is required, if users are required to use a unique Personal Identification Number (PIN), and who selects the PIN?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.2, para 2 c (1) **Logical Access Controls (Authorization/Access Controls)**	Do the access controls for the system: deny access to systems by undefined users or anonymous accounts?	**Interview:**		
FSA ITSPP	4.2, para 2 c (2) **Logical Access Controls (Authorization/Access Controls)**	limit and monitor the usage of administrator and other powerful accounts?	**Interview:**		
FSA ITSPP	4.2, para 2 c (3) **Logical Access Controls (Authorization/Access Controls)**	suspend or delay access capability after a specific number of unsuccessful logon attempts?	**Interview:**		
FSA ITSPP	4.2, para 2 c (4) **Logical Access Controls (Authorization/Access Controls)**	disconnect automatically at the end of a session?	**Interview:**		
FSA ITSPP	4.2, para 2 c (5) **Logical Access Controls (Authorization/Access Controls)**	remove obsolete user accounts as soon as an employee leaves FSA?	**Interview:**		
FSA ITSPP	4.2, para 2 c (6) **Logical Access Controls (Authorization/Access Controls)**	suspend inactive accounts after 90 days?	**Interview:**		
FSA ITSPP	4.2, para 2 c (7) **Logical Access Controls (Authorization/Access Controls)**	remove redundant user IDs, accounts, and role-based accounts from resource access lists?	**Interview:**		
FSA ITSPP	4.2, para 2 c (8) **Logical Access Controls (Authorization/Access Controls)**	protect Audit Logs through strict access controls?	**Interview:**		
FSA ITSPP	4.2, para 2 c (9) **Logical Access Controls (Authorization/Access Controls)**	protect the confidentiality of sensitive information during data transfers and storage?	**Interview:**		
FSA ITSPP	4.2, para 3 **Logical Access Controls (Authorization/Access Controls)**	Is there documentation that describes the specific security controls for hardware and software features that are designed to permit only authorized access to or within an application, its data, or other files?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.2, para 3 **Logical Access Controls (Authorization/Access Controls)**	Is there documentation that describes any restrictions to prevent users from accessing the system or its applications outside of normal work hours or on weekends?	**Documentation Review:** **Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.2, para 3 **Logical Access Controls (Authorization/Access Controls)**	Are there procedures established that address restricting and controlling access to all program libraries, system software, and system hardware?	**Interview:**		
FSA ITSPP	4.2, para 3 **Logical Access Controls (Authorization/Access Controls)**	Is access to security software and hardware restricted to security administrators?	**Interview:** **Visual Inspection:**		
FSA ITSPP	4.2, para 4 **Logical Access Controls (Authorization/Access Controls)**	Has the System Manager assigned a person(s) to review protocols with known vulnerabilities, such as UDP and TFTP, and grant approval for their use prior to implementation?	**Interview:**		
FSA ITSPP	4.2, para 4 **Logical Access Controls (Authorization/Access Controls)**	Does the documentation for the system describe any type of secure gateway or firewall in use, including its configuration?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.2, para 4 **Logical Access Controls (Authorization/Access Controls)**	Do the firewalls meet the standards set forth in the FSA Enterprise Technical Architecture document?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.2, para 4 **Logical Access Controls (Authorization/Access Controls)**	Have system personnel disabled unused system features, services, protocols and ports?	**Interview:**		
FSA ITSPP	4.2, para 4 **Logical Access Controls (Authorization/Access Controls)**	Have system personnel reinitialized all vendor supplied default security parameters to more secure settings?	**Interview:**		
FSA ITSPP	4.2, para 4 **Logical Access Controls (Authorization/Access Controls)**	Does the documentation regarding any port protection devices requiring specific access authorization to the communication ports include the configuration of the port protection devices and whether additional passwords or tokens are required?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.2.1, para 1 **Logical Access Controls (Authorization/Access Controls): Access Control List**	Has the System Manager assigned an employee to create and maintain a current list of authorized users and their access?	**Interview:**		
FSA ITSPP	4.2.1, para 1 **Logical Access Controls (Authorization/Access Controls): Access Control List**	Is this Access Control List (ACL) protected to prevent unauthorized access or viewing of the file?	**Interview:**		
FSA ITSPP	4.2.1, para 1 **Logical Access Controls (Authorization/Access Controls): Access Control List**	Do the person(s) responsible for the ACL remove users who no longer have access rights from the ACL?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.2.1, para 1 **Logical Access Controls (Authorization/Access Controls): Access Control List**	To corroborate this process, do system personnel review ACLs at least every six months to identify and remove users who have left the organization (inactive users), users whose duties no longer require access to the application or system, invalid users, and redundant user IDs and accounts?	**Interview:**		
FSA ITSPP	4.2.2, para 1 **Logical Access Controls (Authorization/Access Controls): Internet or Public Access**	If an application is running on the system that is connected to the Internet or other WAN, have there been additional technical security controls installed to provide protection against unauthorized system penetration?	**Interview:**		
FSA ITSPP	4.2.2, para 1 **Logical Access Controls (Authorization/Access Controls): Internet or Public Access**	Do authorization procedures exist to determine which network and network services are allowed and who is authorized to access them?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.2.2, para 2 **Logical Access Controls (Authorization/Access Controls): Internet or Public Access**	If the public accesses the system, has FSA developed and implemented security controls to protect the integrity of the application and the confidence of the public?	**Interview:**		
FSA ITSPP	4.2.2, para 2 **Logical Access Controls (Authorization/Access Controls): Internet or Public Access**	Does each FSA web page have a designated author or administrator who is responsible for ensuring web page security?	**Interview:**		
FSA ITSPP	4.2.2, para 2 **Logical Access Controls (Authorization/Access Controls): Internet or Public Access**	If a server contains information protected by the Privacy Act, is the information not accessible unless proper authorization is granted?	**Interview:**		
FSA ITSPP	4.2.2, para 2 **Logical Access Controls (Authorization/Access Controls): Internet or Public Access**	Does the website provide notice that it contains Privacy Act information, and give notice of the consequences of unauthorized disclosure?	**Interview:**		
FSA ITSPP	4.2.2, para 2 **Logical Access Controls (Authorization/Access Controls): Internet or Public Access**	Are those users wishing to access the internal system via the Internet authenticated before gaining access?	**Interview:**		
FSA ITSPP	4.2.3, para 1 **Logical Access Controls (Authorization/Access Controls): Remote Access**	Are users who are only authorized to telecommute (i.e., dial-in, VPN, etc.) after he/she has submitted a request to the System Manager, and the System Manager and SSO for the system have reviewed and accepted the request?	**Interview:**		
FSA ITSPP	4.2.3, para 1 **Logical Access Controls (Authorization/Access Controls): Remote Access**	Do the appropriate system personnel monitor all dial-in access?	**Interview:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.3, para 1 **Audit Trails**	Do the audit trail records maintain a log of system and network activity both by system or application processes and by user activity for a minimum of one year?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.3, para 1 **Audit Trails**	In conjunction with appropriate tools and procedures, do the audit trails provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems?	**Interview:**		
FSA ITSPP	4.3, para 2 **Audit Trails**	Is access to audit logs and automated tools strictly controlled and protected against unauthorized changes and/or operational problems?	**Interview:**		
FSA ITSPP	4.3, para 2 **Audit Trails**	In order to access and review audit logs, is the reviewer an appropriate system-level or application-level administrator?	**Interview:**		
FSA ITSPP	4.3, para 2 **Audit Trails**	Are logs reviewed after a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?	**Interview:**		
FSA ITSPP	4.3, para 2 **Audit Trails**	Are automated tools used to help interpret information contained in audit records, discard irrelevant or mundane task information, as well as to distill useful information from the raw data?	**Interview:**		
FSA ITSPP	4.3, para 3 c (1) **Audit Trails**	Do the audit logs include: information on all activity involving access to and modification of sensitive or critical files?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.3, para 3 c (2) **Audit Trails**	sufficient information to establish what events occurred, and who or what caused them?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.3, para 3 c (3) **Audit Trails**	event records that specify: o Type of event; o When the event occurred; o User ID associated with the event; and o Program or command used to initiate the event?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.3, para 3 c (4) **Audit Trails**	records of the number of successful and rejected system access attempts, data access attempts, and other resource access attempts?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.3, para 4 **Audit Trails**	Can the audit logs be queried by user ID, terminal ID, application name, date and time, or some other set of parameters in order to run reports of selected information?	**Interview:**		
FSA ITSPP	4.3, para 4 **Audit Trails**	Are the audit trail clocks synchronized to an agreed upon standard to avoid discrediting the validity of the logs during an investigation?	**Interview:** **Technical Inspection:**		
FSA ITSPP	4.3, para 4 **Audit Trails**	Has the System Manager developed procedures to check and correct any deviations in the time?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.3, para 5 **Audit Trails**	Whenever keystroke monitoring is used, does the SSO document the procedures and provide a means of user notification?	**Documentation Review:** **Interview:**		
FSA ITSPP	4.3, para 5 **Audit Trails**	Do the procedures indicate whether the Department of Justice has reviewed the policy?	**Documentation Review:**		

Document Source	Section Number	Requirement	Test Procedures	Y/N/NA/Waived	Notes
FSA ITSPP	4.3, para 6 **Audit Trails**	Are the duties of FSA security personnel who administer the access control functions and those who administer audit functions segregated?	**Interview:**		